

a manner as to provide visual evidence of unauthorized penetration.

(b) *Doors.* Doors shall be constructed of wood, metal, or other solid material. Entrance doors shall be secured with a built-in GSA-approved three-position combination lock. When special circumstances exist, the agency head may authorize other locks on entrance doors for Secret and Confidential storage. Doors other than those secured with the aforementioned locks shall be secured from the inside with either deadbolt emergency egress hardware, a deadbolt, or a rigid wood or metal bar which extends across the width of the door, or by other means approved by the agency head.

(c) *Vents, ducts, and miscellaneous openings.* All vents, ducts, and similar openings in excess of 96 square inches (and over 6 inches in its smallest dimension) that enter or pass through an open storage area shall be protected with either bars, expanded metal grills, commercial metal sound baffles, or an intrusion detection system.

(d) *Windows.* (1) All windows which might reasonably afford visual observation of classified activities within the facility shall be made opaque or equipped with blinds, drapes, or other coverings.

(2) Windows within 18 feet of the ground will be constructed from or covered with materials which provide protection from forced entry. The protection provided to the windows need be no stronger than the strength of the contiguous walls. Open storage areas which are located within a controlled compound or equivalent may eliminate the requirement for forced entry protection if the windows are made inoperable either by permanently sealing them or equipping them on the inside with a locking mechanism and they are covered by an IDS (either independently or by the motion detection sensors within the area).

§ 2001.54 Foreign government information.

The requirements described below are additional baseline safeguarding standards that may be necessary for foreign government information, other than NATO information, that requires protection pursuant to an existing treaty,

agreement, bilateral exchange or other obligation. NATO classified information shall be safeguarded in compliance with USSAN 1-07. To the extent practical, and to facilitate its control, foreign government information should be stored separately from other classified information. To avoid additional costs, separate storage may be accomplished by methods such as separate drawers of a container. The safeguarding standards described in paragraphs (a) through (e) of this section may be modified if required or permitted by treaties or agreements, or for other obligations, with the prior written consent of the National Security Authority of the originating government, hereafter “originating government.”

(a) *Top Secret.* Records shall be maintained of the receipt, internal distribution, destruction, access, reproduction, and transmittal of foreign government Top Secret information. Reproduction requires the consent of the originating government. Destruction will be witnessed.

(b) *Secret.* Records shall be maintained of the receipt, external dispatch and destruction of foreign government Secret information. Other records may be necessary if required by the originator. Secret foreign government information may be reproduced to meet mission requirements unless prohibited by the originator. Reproduction shall be recorded unless this requirement is waived by the originator.

(c) *Confidential.* Records need not be maintained for foreign government Confidential information unless required by the originator.

(d) *Restricted and other foreign government information provided in confidence.* In order to assure the protection of other foreign government information provided in confidence (e.g., foreign government “Restricted,” “Designated,” or unclassified provided in confidence), such information must be classified under the Order. The receiving agency, or a receiving U.S. contractor, licensee, grantee, or certificate holder acting in accordance with instructions received from the U.S. Government, shall provide a degree of protection to the foreign government information at least equivalent to that

required by the government or international organization that provided the information. When adequate to achieve equivalency, these standards may be less restrictive than the safeguarding standards that ordinarily apply to U.S. Confidential information. If the foreign protection requirement is lower than the protection required for U.S. Confidential information, the following requirements shall be met:

(1) Documents may retain their original foreign markings if the responsible agency determines that these markings are adequate to meet the purposes served by U.S. classification markings. Otherwise, documents shall be marked, “This document contains (insert name of country) (insert classification level) information to be treated as U.S. (insert classification level).” The notation, “Modified Handling Authorized,” may be added to either the foreign or U.S. markings authorized for foreign government information. If remarking foreign originated documents or matter is impractical, an approved cover sheet is an authorized option;

(2) Documents shall be provided only to persons in accordance with sections 4.1(a) and (h) of the Order;

(3) Individuals being given access shall be notified of applicable handling instructions. This may be accomplished by a briefing, written instructions, or by applying specific handling requirements to an approved cover sheet;

(4) Documents shall be stored in such a manner so as to prevent unauthorized access;

(5) Documents shall be transmitted in a method approved for classified information, unless this method is waived by the originating government.

(e) *Third-country transfers.* The release or disclosure of foreign government information to any third-country entity must have the prior consent of the originating government if required by a treaty, agreement, bilateral exchange, or other obligation.

§ 2001.55 Foreign disclosure of classified information.

Classified information originating in one agency may be disseminated by any other agency to which it has been made available to a foreign govern-

ment or international organization of governments, or any element thereof, in accordance with statute, the Order, directives implementing the Order, direction of the President, or with the consent of the originating agency, unless the originating agency has determined that prior authorization is required for such dissemination and has marked or indicated such requirement on the medium containing the classified information. Markings used to implement this section shall be approved in accordance with § 2001.24(j). With respect to the Intelligence Community, the Director of National Intelligence may issue policy directives or guidelines pursuant to section 6.2(b) of the Order that modify such prior authorization.

Subpart F—Self-Inspections

§ 2001.60 General.

(a) *Purpose.* This subpart sets standards for establishing and maintaining an ongoing agency self-inspection program, which shall include regular reviews of representative samples of the agency’s original and derivative classification actions.

(b) *Responsibility.* The senior agency official is responsible for directing and administering the agency’s self-inspection program. The senior agency official shall designate agency personnel to assist in carrying out this responsibility. The program shall be structured to provide the senior agency official with information necessary to assess the effectiveness of the classified national security information program within individual agency activities and the agency as a whole, in order to enable the senior agency official to fulfill his or her responsibility to oversee the agency’s program under section 5.4(d) of the Order.

(c) *Approach.* The senior agency official shall determine the means and methods for the conduct of self-inspections.

(1) Self-inspections should evaluate the adherence to the principles and requirements of the Order and this directive and the effectiveness of agency